(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－136234

(43)公開日　平成11年(1999)５月21日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｃ
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｅ
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｅ
			６４０Ｂ

審査請求　有　　請求項の数６　ＯＬ　（全７頁）

(21)出願番号　特願平9－298913

(22)出願日　平成９年(1997)10月30日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　井田　雄二
東京都港区芝五丁目７番１号　日本電気株式会社内

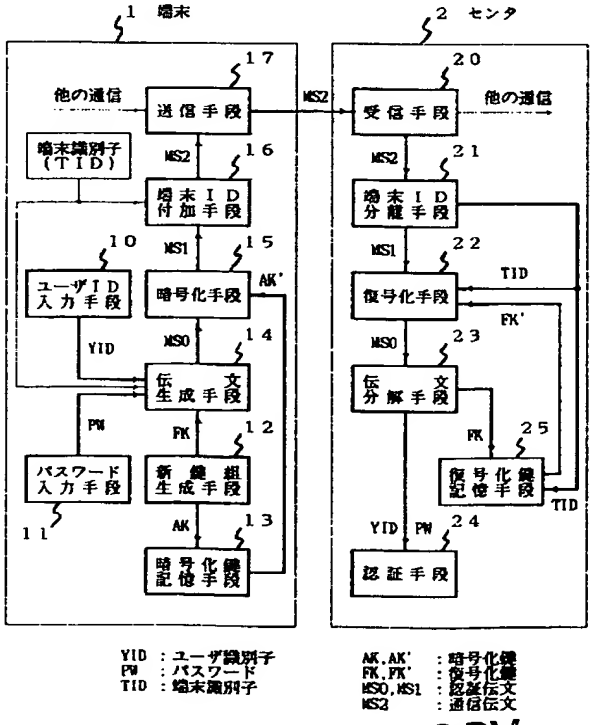
(74)代理人　弁理士　京本　直樹　（外２名）

(54)【発明の名称】　利用者認証方式および利用者認証方法

(57)【要約】

【課題】使用する暗号化鍵，復号化鍵をその都度変更し、端末，センタ間のユーザ認証を往復プロトコルを用いず安全に行い、再送攻撃にも対応可能とする。

【解決手段】端末１の新鍵組生成手段１２は暗号化鍵と復号化鍵の組を多数持ち認証要求の都度ランダムに一組を選択する。暗号化鍵記憶手段１３には前回選択した暗号化鍵ＡＫ’が保持されており、ユーザ識別子ＹＩＤ，パスワードＰＷ，端末識別子ＴＩＤに今回選択した復号化鍵ＦＫを加えた伝文を暗号化手段１５でＡＫ’で暗号化し、平文のＴＩＤを付加して送信する。センタ２の復号化鍵記憶手段２５にはＴＩＤごとに前回送られてきた復号化鍵ＦＫ’が記憶されており、復号化手段２２は端末ＩＤ分離手段２１で分離したＴＩＤで取得したＦＫ’で復号を行い、平文で送られてきＴＩＤと復号したＴＩＤの一致を確認し、ユーザ認証を行い今回送られてきた復号化鍵ＦＫで暗号化鍵記憶手段１３を更新する。



1

【特許請求の範囲】

【請求項１】　ユーザ識別子とパスワードとを端末からセンタに送信し、センタの登録情報と比較してユーザ認証を行う利用者認証方式において、前記端末に、認証要求時に多数の暗号化鍵と復号化鍵との組の中からランダムに一組を選択する新鍵組生成手段と、前記新鍵組生成手段が選択した暗号化鍵と復号化鍵の組の中の暗号化鍵を少なくとも次回の認証要求時まで保持する暗号化鍵記憶手段と、ユーザ識別子，パスワードに復号確認用固有ワード及び前記新鍵組生成手段が選択した暗号化鍵と復号化鍵の組の中の復号化鍵を付加して認証伝文を作成する伝文生成手段と、前記伝文生成手段が作成した認証伝文を前記暗号化鍵記憶手段に記憶されている前回の認証要求時に選択された暗号化鍵で暗号化する暗号化手段と、前記暗号化手段の出力に端末識別子を付加して通信伝文を生成する端末ＩＤ付加手段とを備え、前記センタには、前記端末から送信された復号化鍵を次回認証要求時に使用する復号化鍵として端末識別子別に記憶しておく復号化鍵記憶手段と、受信した通信伝文から端末識別子を分離する端末ＩＤ分離手段と、前記端末ＩＤ分離手段で分離した端末識別子により前記復号化鍵記憶手段から前回の認証要求時に記憶した復号化鍵を取得して暗号化された認証伝文を復号し復号確認用固有ワードにより復号の正否を確認する復号化手段と、復号が正常に行われたとき復号された認証伝文を分解して得られた復号化鍵で前記復号化鍵記憶手段を更新しユーザ識別子とパスワードとをユーザ認証用に出力する伝文分解手段と、前記伝文分解手段からのユーザ識別子とパスワードとを登録情報と比較してユーザ認証を行う認証手段とを備えたことを特徴とする利用者認証方式。

【請求項２】　前記伝文生成手段においてユーザ識別子，パスワードに付加する復号確認用固有ワードとして端末識別子を使用したことを特徴とする請求項１記載の利用者認証方式。

【請求項３】　前記新鍵組生成手段が同一の暗号化鍵と復号化鍵との組を連続して選択することを抑止する機能を有することを特徴とする請求項１又は請求項２記載の利用者認証方式。

【請求項４】　端末の前記新鍵組生成手段と伝文生成手段との間に前記新鍵組生成手段で選択された復号化鍵をセンタ固有の暗号化鍵で暗号化する復号化鍵暗号化手段を有し、センタの前記伝文分解手段と復号化鍵記憶手段との間に前記伝文分解手段から出力される端末の前記復号化鍵暗号化手段で暗号化された復号化鍵をセンタ固有の復号化鍵で復号する復号化鍵復号化手段を有することを特徴とする請求項１，請求項２又は請求項３記載の利用者認証方式。

【請求項５】　前記復号化鍵暗号化手段が使用するセンタ固有の暗号化鍵は公開鍵方式の公開鍵であり、前記復号化鍵復号化手段が使用する復号化鍵は公開鍵方式の秘

2

密鍵であることを特徴とする請求項４記載の利用者認証方式。

【請求項６】　ユーザ識別子とパスワードとを端末からセンタに送信し、センタの登録情報と比較してユーザ認証を行う利用者認証方法において、前記端末では、認証要求時に多数の暗号化鍵と復号化鍵との組の中からランダムに一組を選択し、選択した暗号化鍵を少なくとも次回の認証要求時まで保持すると共に、復号確認用固有ワードと選択した復号化鍵とをユーザ識別子，パスワードに付加した認証伝文を作成し、この認証伝文を前回の認証要求時に選択し記憶しておいた暗号化鍵を用いて暗号化し、暗号化した認証伝文に端末識別子を付加した通信伝文を送信し、これを受信した前記センタでは、受信した通信伝文から端末識別子を分離し、分離した端末識別子により前回の認証要求時に記憶した復号化鍵を取得して暗号化された認証伝文を復号し、復号確認用固有ワードにより復号の正否を確認し、復号が正常に行われていた場合に認証伝文の中の復号化鍵を次回の同一端末からの認証要求時に使用する復号化鍵として記憶し、復号されたユーザ識別子とパスワードとを登録情報と比較してユーザ認証を行うことを特徴とする利用者認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は利用者認証方式および利用者認証方法に関し、特にネットワークを介して端末，センタ間で往復のプロトコルを用いず安全にユーザ認証を行う利用者認証方式および利用者認証方法に関する。

【０００２】

【従来の技術】近年の分散処理環境では、ユーザが端末からネットワークを介してセンタの資源を利用したり操作したりすることが多く、センタ側で端末からの要求に対して利用権，操作権の確認のためユーザ認証を行う必要がある。従来、この種のユーザ認証には、端末側からユーザ識別子とパスワードとを平文もしくは固定的な暗号化を行ってセンタ側に一方通行のプロトコルで送信し、センタ側でパスワードを確認してユーザ認証を行うのが一般的な方法である。

【０００３】しかしながら、平文でユーザ識別子とパスワードとを送信する場合は、通信経路の途中で盗聴されるとパスワードが漏洩し悪用される恐れがある。固定的な暗号化を行って送信する場合には、盗聴されてもパスワードが漏洩し悪用されることを防止できるが、盗聴した信号を記録しておき、後刻そのまま再送してシステムを混乱させる再送攻撃に対しては無防備であるという欠点がある。

【０００４】これに対して、特開平７－３２５７８５号公報には、往復プロトコルを使用することにより、上述の再送攻撃を無効とする認証方法が開示されている。この方法では、端末からの認証要求に対してセンタ側で乱

数を発生して端末側に送信する。端末では、ユーザ識別子とパスワードとに受信した乱数を含めて暗号化してセンタ側に再び送信する。センタ側では、送信された暗号文を復号して先に送信した乱数値と比較して一致したとき、ユーザ識別子とパスワードとによるユーザ認証を行う。この方法によれば、認証を行う度に乱数が異なるため、盗聴によるパスワードの漏洩を防止すると共に再送攻撃を無効とすることができる。

【０００５】

【発明が解決しようとする課題】しかしながら、上述した特開平７－３２５７８５号公報記載の方法は、往復プロトコルを使用するため、双方向の通信が可能な装置構成が不可欠であり、双方向ともに大きな通信容量が必要となる。特にセンタに多数の端末が接続されている場合には、センタ側の負担が大きくなるという問題点がある。

【０００６】本発明の目的は、以上の問題点を解決し、端末，センタ間のユーザ認証を往復プロトコルを用いずに安全に行え、且つ再送攻撃にも対応できる利用者認証方式および利用者認証方法を提供することにある。

【０００７】

【課題を解決するための手段】請求項１の利用者認証方式は、ユーザ識別子とパスワードとを端末からセンタに送信し、センタの登録情報と比較してユーザ認証を行う利用者認証方式において、前記端末に、認証要求時に多数の暗号化鍵と復号化鍵との組の中からランダムに一組を選択する新鍵組生成手段と、前記新鍵組生成手段が選択した暗号化鍵と復号化鍵の組の中の暗号化鍵を少なくとも次回の認証要求時まで保持する暗号化鍵記憶手段と、ユーザ識別子，パスワードに復号確認用固有ワード及び前記新鍵組生成手段が選択した暗号化鍵と復号化鍵の組の中の復号化鍵を付加して認証伝文を作成する伝文生成手段と、前記伝文生成手段が作成した認証伝文を前記暗号化鍵記憶手段に記憶されている前回の認証要求時に選択された暗号化鍵で暗号化する暗号化手段と、前記暗号化手段の出力に端末識別子を付加して通信伝文を生成する端末ＩＤ付加手段とを備え、前記センタには、前記端末から送信された復号化鍵を次回認証要求時に使用する復号化鍵として端末識別子別に記憶しておく復号化鍵記憶手段と、受信した通信伝文から端末識別子を分離する端末ＩＤ分離手段と、前記端末ＩＤ分離手段で分離した端末識別子により前記復号化鍵記憶手段から前回の認証要求時に記憶した復号化鍵を取得して暗号化された認証伝文を復号し復号確認用固有ワードにより復号の正否を確認する復号化手段と、復号が正常に行われたとき復号された認証伝文を分解して得られた復号化鍵で前記復号化鍵記憶手段を更新しユーザ識別子とパスワードとをユーザ認証用に出力する伝文分解手段と、前記伝文分解手段からのユーザ識別子とパスワードとを登録情報と比較してユーザ認証を行う認証手段とを備えて構成されている。

【０００８】請求項２の利用者認証方式は、請求項１記載の利用者認証方式において、前記伝文生成手段においてユーザ識別子，パスワードに付加する復号確認用固有ワードとして端末識別子を使用したことを特徴としている。

【０００９】請求項３の利用者認証方式は、請求項１又は請求項２記載の利用者認証方式において、前記新鍵組生成手段が同一の暗号化鍵と復号化鍵との組を連続して選択することを抑止する機能を有することを特徴としている。

【００１０】請求項４の利用者認証方式は、請求項１，請求項２又は請求項３記載の利用者認証方式において、端末の前記新鍵組生成手段と伝文生成手段との間に前記新鍵組生成手段で選択された復号化鍵をセンタ固有の暗号化鍵で暗号化する復号化鍵暗号化手段を有し、センタの前記伝文分解手段と復号化鍵記憶手段との間に前記伝文分解手段から出力される端末の前記復号化鍵暗号化手段で暗号化された復号化鍵をセンタ固有の復号化鍵で復号する復号化鍵復号化手段を有することを特徴としている。

【００１１】請求項５の利用者認証方式は、請求項４記載の利用者認証方式において、前記復号化鍵暗号化手段が使用するセンタ固有の暗号化鍵は公開鍵方式の公開鍵であり、前記復号化鍵復号化手段が使用する復号化鍵は公開鍵方式の秘密鍵であることを特徴としている。

【００１２】請求項６の利用者認証方法は、ユーザ識別子とパスワードとを端末からセンタに送信し、センタの登録情報と比較してユーザ認証を行う利用者認証方法において、前記端末では、認証要求時に多数の暗号化鍵と復号化鍵との組の中からランダムに一組を選択し、選択した暗号化鍵を少なくとも次回の認証要求時まで保持すると共に、復号確認用固有ワードと選択した復号化鍵とをユーザ識別子，パスワードに付加した認証伝文を作成し、この認証伝文を前回の認証要求時に選択し記憶しておいた暗号化鍵を用いて暗号化し、暗号化した認証伝文に端末識別子を付加した通信伝文を送信し、これを受信した前記センタでは、受信した通信伝文から端末識別子を分離し、分離した端末識別子により前回の認証要求時に記憶した復号化鍵を取得して暗号化された認証伝文を復号し、復号確認用固有ワードにより復号の正否を確認し、復号が正常に行われていた場合に認証伝文の中の復号化鍵を次回の同一端末からの認証要求時に使用する復号化鍵として記憶し、復号されたユーザ識別子とパスワードとを登録情報と比較してユーザ認証を行うことを特徴としている。

【００１３】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して説明する。

【００１４】図１は本発明の第１の実施の形態の構成を

示すブロック図である。

【００１５】第１の実施の形態の利用者認証方式は、図１に示すように、端末１とセンタ２との間でユーザ認証を行うものであり、端末１は、ユーザＩＤ入力手段１０，パスワード入力手段１１，新鍵組生成手段１２，暗号化鍵記憶手段１３，伝文生成手段１４，暗号化手段１５，端末ＩＤ付加手段１６及び送信手段１７から構成され、センタ２は、受信手段２０，端末ＩＤ分離手段２１，復号化手段２２，伝文分解手段２３，認証手段２４及び復号化鍵記憶手段２５で構成されている。

【００１６】端末１の新鍵組生成手段１２は、多数の暗号化鍵と復号化鍵の組を記憶しており、端末１から認証要求を行う場合に、これらの多数組の中からランダムに一組の暗号化鍵ＡＫと復号化鍵ＦＫとの組を選択して出力する。

【００１７】暗号化鍵記憶手段１３は、送信手段１７から通信伝文ＭＳ２をセンタ２に送信した後、新鍵組生成手段１２が選択した暗号化鍵ＡＫと復号化鍵ＦＫの組の中から暗号化鍵ＡＫを記憶し、次回の認証要求時まで保持する不揮発性のメモリである。なお、通信伝文ＭＳ２が送信されるまでは、前回の認証要求時に記憶した暗号化鍵ＡＫ’が記憶されており、今回の認証要求時の暗号化に使用される。

【００１８】伝文生成手段１４は、ユーザＩＤ入力手段１０で入力したユーザ識別子ＹＩＤ及びパスワード入力手段１１で入力したパスワードＰＷに、新鍵組生成手段１２が選択した復号化鍵ＦＫと端末識別子ＴＩＤとを合成し、認証伝文ＭＳ０を生成する。

【００１９】暗号化手段１５は、伝文生成手段１４で生成された認証伝文ＭＳ０を暗号化鍵記憶手段１３に前回の認証要求時に記憶されて保存されている暗号化鍵ＡＫ’を用いて暗号化する。

【００２０】端末ＩＤ付加手段１６は、暗号化手段１５で暗号化された認証伝文ＭＳ１に端末識別子ＴＩＤと認証要求を示す識別符号とを付加し、通信伝文ＭＳ２を生成する。

【００２１】送信手段１７は、端末ＩＤ付加手段１６で作成された通信伝文ＭＳ２をネットワークを介してセンタ２に送信する。

【００２２】センタ２の受信手段２０は、端末１から送信された通信伝文ＭＳ２を受信し、認証要求であることを認識すると、受信した通信伝文ＭＳ２を端末ＩＤ分離手段２１に渡す。

【００２３】端末ＩＤ分離手段２１は、受け取った通信伝文ＭＳ２から端末識別子ＴＩＤを分離して取り出すと共に、端末識別子ＴＩＤと認証要求を示す識別符号とを除いた暗号化された認証伝文ＭＳ１を復号化手段２２に渡す。

【００２４】復号化手段２２は、端末ＩＤ分離手段２１で取り出した端末識別子ＴＩＤにより復号化鍵記憶手段２５から抽出した端末識別子ＴＩＤ用の復号化鍵ＦＫ’を使用し、暗号化された認証伝文ＭＳ１を復号する。その後、復号して得られた端末識別子ＴＩＤと端末ＩＤ分離手段２１で分離した端末識別子ＴＩＤとを比較し、両者が一致した場合、復号した認証伝文ＭＳ０を伝文分解手段２３に渡す。

【００２５】伝文分解手段２３は、復号化手段２２からの復号された認証伝文ＭＳ０を分解し、ユーザ識別子ＹＩＤ，パスワードＰＷを認証手段２４に、復号化鍵ＦＫを復号化鍵記憶手段２５に出力する。

【００２６】認証手段２４は、伝文分解手段２３から入力されるユーザ識別子ＹＩＤとパスワードＰＷとを用い、登録情報との照合によりユーザ認証を行う。

【００２７】復号化鍵記憶手段２５は、端末から送信された復号化鍵を次回の認証要求時に使用する復号化鍵として端末識別子別に記憶し保持している不揮発性のメモリであり、伝文分解手段２３から入力された復号化鍵ＦＫを、端末識別子ＴＩＤ用の次回の認証要求時に使用する復号化鍵として記憶する。なお、復号化鍵ＦＫが記憶されるまでは、前回の認証要求時に記憶された復号化鍵ＦＫ’が記憶されており、今回の認証要求時の復号に使用される。

【００２８】次に、上述のように構成された本実施の形態の動作を詳細に説明する。まず、端末１から正常に認証要求が行われた場合の動作について説明する。

【００２９】端末１において、ユーザＩＤ入力手段１０によりユーザ識別子ＹＩＤを、パスワード入力手段１１によりパスワードＰＷをそれぞれ入力し、認証要求の送信を指示する。これを受けて、新鍵組生成手段１２は、暗号化鍵ＡＫと復号化鍵ＦＫとを生成し復号化鍵ＦＫを伝文生成手段１４に送る。伝文生成手段１４は、ユーザ識別子ＹＩＤ，パスワードＰＷ，復号化鍵ＦＫ及び端末識別子ＴＩＤで認証伝文ＭＳ０を作成し、暗号化手段１５に送る。暗号化手段１５は、その時点で暗号化鍵記憶手段１３に記憶されている暗号化鍵ＡＫ’を取得して認証伝文ＭＳ０を暗号化する。暗号化された認証伝文ＭＳ１に、端末ＩＤ付加手段１６で端末識別子ＴＩＤと認証要求であることを示す識別符号とが付加され、通信伝文ＭＳ２として送信手段１７からセンタ２に送信される。送信が行われると、新鍵組生成手段１２で生成された暗号化鍵ＡＫは、次回用の暗号化鍵として暗号化鍵記憶手段１３に記憶される。

【００３０】センタ２では、受信手段２０が端末１から送信された通信伝文ＭＳ２を受信して、認証要求であると判断すると端末ＩＤ分離手段２１に送る。端末ＩＤ分離手段２１は、通信伝文ＭＳ２から端末識別子ＴＩＤを分離し、残りの暗号化された認証伝文ＭＳ１を復号化手段２２に渡す。分離した端末識別子ＴＩＤは、復号化手段２２及び復号化鍵記憶手段２５に通知される。この時点では、復号化鍵記憶手段２５には端末１からの前回の

認証要求時に格納された復号化鍵ＦＫ’が記憶されている。復号化手段２２は、復号化鍵記憶手段２５からこの復号化鍵ＦＫ’を取得し、暗号化された認証伝文ＭＳ１を復号化鍵ＦＫ’で復号する。そして、復号した認証伝文ＭＳ０中の端末識別子ＴＩＤと端末ＩＤ分離手段２１から渡された端末識別子ＴＩＤとを照合し、両者が一致することを確認すると復号した認証伝文ＭＳ０を伝文分解手段２３に渡す。伝文分解手段２３は、認証伝文ＭＳ０を分解してユーザ識別子ＹＩＤとパスワードＰＷとを認証手段２４に、復号化鍵ＦＫを復号化鍵記憶手段２５にそれぞれ出力する。認証手段２４は、受け取ったユーザ識別子ＹＩＤ及びパスワードＰＷをあらかじめ登録されている登録情報と比較してユーザ認証を行う。復号化鍵記憶手段２５は、受け取った復号化鍵ＦＫを端末識別子ＴＩＤ用の次回使用する復号化鍵として、それまで格納されていた復号化鍵ＦＫ’に代えて記憶し保存する。

【００３１】以上により、往復のプロトコルを使用することなく、一方向のみのプロトコルにより、その都度使用する暗号化鍵と復号化鍵の組み合わせを変更してユーザ認証を行うことができる。従って、盗聴によりパスワードが漏洩する可能性は著しく低減されると共に、盗聴した信号をそのまま再送してシステムを混乱させる再送攻撃に対しても対応することができる。以下、再送攻撃に対する動作について説明する。

【００３２】まず、端末１とセンタ２の間で暗号化された通信伝文ＭＳ２が第三者により盗聴され、間を置かず再送された場合を考える。第三者が盗聴している間に、通信伝文ＭＳ２はセンタ２において正常に復号化鍵記憶手段２５に記憶されていた復号化鍵ＦＫ’により復号処理され、復号化鍵記憶手段２５の記憶内容は通信伝文ＭＳ２で転送されてきた復号化鍵ＦＫに置き換えられている。従って、再送された不正な通信伝文は正常に復号されず、復号化手段２２は端末識別子ＴＩＤの不一致のため処理を中断し、認証手段２４によるユーザ認証は行われず、復号化鍵記憶手段２５には復号化鍵ＦＫが記憶されたままとなる。すなわち、次に端末１から正常な認証要求が行われた場合には、正常な動作が行える。なお、盗聴した通信伝文を間を置いて後刻再送した場合でも、暗号化鍵と復号化鍵の組が多数の中からランダムに選択され、正常な認証要求の度に変更されるので、盗聴時の暗号化鍵と再送攻撃時の復号化鍵とが整合して正常な復号が行われる可能性は極めて低い。

【００３３】以上の説明では、センタで正常な復号が行われたことを確認するために、端末から平文のままの端末識別子と暗号化した端末識別子とを重複して送信するものとした。しかしながら、センタにおける正常な復号を確認するためには、センタで復号を行わずに取得できる決められた固有ワードを復号確認用ワードとして端末から暗号化して送ればよい。すなわち、端末から暗号化して送信する復号確認用ワードは、上述した端末識別子に限られず、センタにあらかじめ登録した端末別の固有ワードでも、全端末に対して共通の一つの固有ワードでもよい。

【００３４】又、端末の新鍵組生成手段では暗号化鍵と復号化鍵との組をランダムに生成するとのみ述べたが、第三者による再送攻撃は間を置かずに行われることが多いと思われるので、同じ暗号化鍵と復号化鍵との組を連続して選択しないように、同一組の連続選択を抑止する機能を付加すると、再送攻撃に対する安全性が更に確実となる。なお、新鍵組生成手段が持つ暗号化鍵と復号化鍵との組の数は、多いほど再送攻撃に対する安全性が増す。これらの暗号化鍵と復号化鍵との組は、複数の端末がセンタに接続される場合に、端末別に異なる必要はなく全端末に共通であっても差し支えない。

【００３５】更に、端末の暗号化鍵記憶手段には、新鍵組生成手段で選択した暗号化鍵を次回の認証要求時まで保持しておくよう説明した。端末から送信された伝文がセンタで受信される場合は、これで十分である。しかし、送信した伝文が通信経路の障害でセンタで受信できない場合を考慮すると、暗号化鍵記憶手段にはランダムに選択した暗号化鍵を次回まででなく、次の次の回まで保持するようにすることが望ましい。すなわち、暗号化鍵記憶手段には前回に選択された暗号化鍵と前々回に選択した暗号化鍵とを記憶し、伝文未達時に再送する際には、前回ではなく前々回に選択した暗号化鍵を使用するようにすると、通信経路障害による未達時の再送処理が容易となる。

【００３６】図２は、本発明の第２の実施の形態の構成を示すブロック図である。

【００３７】図２に示す本発明の第２の実施の形態は、端末１ａとセンタ２ａから成り、図１の第１の実施の形態と相違する点は、端末１ａの新鍵組生成手段１２と伝文生成手段１４との間に、センタ固有の暗号化鍵で新鍵組生成手段１２が選択した復号化鍵ＦＫを暗号化して復号化鍵ＦＫ”とする復号化鍵暗号化手段１８が挿入され、センタ２ａの伝文分解手段２３と復号化鍵記憶手段２５との間には、伝文分解手段２３から出力される暗号化された復号化鍵ＦＫ”をセンタ固有の復号化鍵で復号する復号化鍵復号化手段２６が挿入されていることである。

【００３８】上述した端末１ａの復号化鍵暗号化手段１８とセンタ２ａの復号化鍵復号化手段２６とを除く各手段の構成と動作は、図１の第１の実施の形態の場合と同じであり、送信伝文ＭＳ２に含まれる復号化鍵が二重に暗号化されているため、盗聴により情報が漏洩する可能性がより少なくなる利点がある。

【００３９】なお、復号化鍵を二重に暗号化するための暗号化方式は特に限定されるものではなく、共通鍵方式でも公開鍵方式でもよいが、暗号化鍵を公開鍵方式の公開鍵とし、復号化鍵は秘密鍵としてセンタで管理するの

がよい。この秘密鍵は端末別に設定して復号化鍵記憶手段２５に格納し、端末識別子により該当するものを復号化手段２２の復号化鍵ＦＫ’と同様に読み出すようにしてもよく、全端末に共通として復号化鍵復号化手段２６内に記憶させるようにしてもよい。

【００４０】以上、図面を参照して第１及び第２の実施の形態について説明したが、両者に共通する処理手順は、下記のように要約することができる。すなわち、端末は多数の暗号化鍵と復号化鍵との組を記憶しており、認証要求時にその中からランダムに一組を選択し、選択した暗号化鍵を次回の認証要求時まで保持すると共に、端末識別子と選択した復号化鍵とをユーザ識別子，パスワードに付加した後、前回の認証要求時に選択し記憶しておいた暗号化鍵で暗号化し、端末識別子を付加して送信する。これを受信したセンタでは、端末識別子を分離し、分離した端末識別子により前回の認証要求時に記憶しておいた復号化鍵を取得して復号し、復号した端末識別子を分離した端末識別子と照合して復号の正否を確認し、復号が正常に行われていた場合に復号した復号化鍵を同一端末からの次回の認証要求時に使用するために記憶した後、復号されたユーザ識別子とパスワードとでユーザ認証を行う。

【００４１】

【発明の効果】以上説明したように、本発明の利用者認証方式および利用者認証方法は、端末側に多数の暗号化鍵と復号化鍵の組を持ち、認証要求の度にその中から一組をランダムに選択し、今回選択した組は次回用として暗号化鍵を端末で記憶し復号化鍵は暗号化して送信しセンタに記憶させ、今回の暗号処理には前回選択され端末およびセンタに記憶されている暗号化鍵と復号化鍵の組を使用するよう構成されている。これにより、認証要求の度に異なる暗号化鍵，復号化鍵が使用されることになり、往復プロトコルを使用することなく安全な認証が行え、且つ第三者による再送攻撃にも対応することができる。この結果、双方向性を持たない若しくは持つことが困難な端末からの安全な認証が可能となると共に、認証に必要な通信容量の削減もでき、多数の端末が接続されている場合でもセンタ側の負担が軽くなる効果がある。

【００４２】又、端末で生成した次回使用する復号化鍵を正当なセンタのみが復号化可能な暗号化鍵で暗号化することにより、より安全に端末ごとの復号化鍵の情報をセンタに送信することができる。

【図面の簡単な説明】

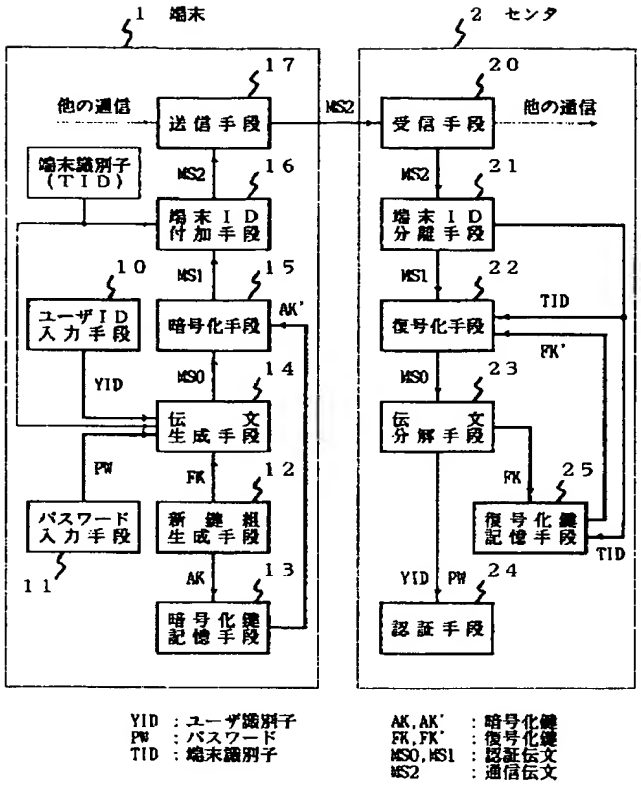
【図１】本発明の第１の実施の形態の構成を示すブロック図である。

【図２】本発明の第２の実施の形態の構成を示すブロック図である。

【符号の説明】

１，１ａ　端末
２，２ａ　センタ
１０　ユーザＩＤ入力手段
１１　パスワード入力手段
１２　新鍵組生成手段
１３　暗号化鍵記憶手段
１４　伝文生成手段
１５　暗号化手段
１６　端末ＩＤ付加手段
１７　送信手段
１８　復号化鍵暗号化手段
２０　受信手段
２１　端末ＩＤ分離手段
２２　復号化手段
２３　伝文分解手段
２４　認証手段
２５　復号化鍵記憶手段
２６　復号化鍵復号化手段

【図１】



【図２】